CLAIMS

What is claimed is:

1. A system for controlling access to computing resources within an enterprise comprising:

   a web server and a web security agent controlling access to Uniform Resource Locators (URLs);

   a security gatekeeper and an access server controlling access to Application Programming Interfaces (APIs); and

   a core security framework used by both the web server and web security agent and the security gatekeeper and access server to store security data and policies and approve or deny requests for access to URLs and APIs.

2. The system of claim 1 wherein the access server is a Standard Object Access Protocol (SOAP) server.

3. The system of claim 1 wherein the core security framework comprises a policy store, a data store, and a policy server.

4. The system of claim 3 wherein the data store is a relational database.

5. The system of claim 3 wherein the data store is a directory.

6. The system of claim 1 wherein, upon the core security framework approving a request for access to an API, the core security framework creates a session token and attaches the session

token to the approved request, the session token providing access to the API for the duration of a session.

7. A system for communication between two independent computing domains comprising:

a security gatekeeper within the second domain to intercept an invocation from the first domain to an API in the second domain;

a core security framework coupled to the security gatekeeper wherein the security gatekeeper sends security-related information in the invocation to the core security framework, the core security framework authenticates an entity making the invocation and authorizes the entity to invoke the API, and the core security framework informs the security gatekeeper that the entity making the invocation has been authenticated and authorized; and

an access server coupled to the security gatekeeper wherein the security gatekeeper informs the access server that the entity making the invocation has been authenticated and authorized and the access server provides the entity making the invocation with access to the API;

wherein the core security framework is also used to control access to URLs within the second domain.

8. The system of claim 7 wherein the core security framework comprises a policy store, a data store, and a policy server.

9. The system of claim 8 wherein the data store is a relational database.

10. The system of claim 8 wherein the data store is a directory.

11. The system of claim 7 wherein a session token is created that provides an entity invoking an API with access to the API for the duration of a session.

12. The system of claim 7 wherein communications between the first domain and the second domain are in a format compliant with SOAP.

13. The system of claim 12 wherein the security gatekeeper intercepts all data transmissions from the first domain to the second domain that are in the SOAP format.

14. The system of claim 7 wherein the API invocation from the first domain is a request to authenticate and authorize a user within the second domain seeking access to data within the first domain.

15. A method of communicating between two independent computing domains comprising:

a user within the first domain sending to the second domain a SOAP-compliant data request that also contains security-related information;

a security gatekeeper within the second domain intercepting the data request;

the security gatekeeper sending the data request to a core security framework within the second domain;

the core security framework using the security-related information in the data request to authenticate the user and authorize the user to retrieve the requested data;

the core security framework returning the data request to the security gatekeeper and informing the security gatekeeper that the user has been authenticated and authorized;

the security gatekeeper sending the data request to a SOAP server and informing the SOAP server that the user has been authenticated and authorized; and

the SOAP server providing the user with access to the requested data;

wherein the core security framework is also used to control access to URLs within the second domain.

16. The method of claim 15 wherein the data request is a request for access to an API within the second domain.

17. The method of claim 15 wherein the core security framework comprises a policy store, a data store, and a policy server.

18. The method of claim 17 wherein the data store is a relational database.

19. The method of claim 17 wherein the data store is a directory.

20. The method of claim 15 wherein a session token is created that provides the user with access to the requested data for the duration of the session.

21. The method of claim 15 wherein data requests from the user and data returned to the user are in a format compliant with SOAP.

22. The method of claim 21 wherein all data transmissions from the first domain to the second domain that are in the SOAP format are intercepted by the security gatekeeper.

23. The method of claim 15 wherein the data request from the first domain is a request to authenticate and authorize a user within the second domain seeking access to data within the first domain.

24. A method for a user within a first enterprise to gain access to data within a second enterprise comprising:

the user logging in to a secure computing domain within the first enterprise;

the user requesting data from the second enterprise;

the first enterprise adding security information to the data request and sending the data request and security information to the second enterprise;

a security gatekeeper within the second enterprise intercepting the security information;

the security gatekeeper sending the security information to a core security framework within the second enterprise;

the second enterprise's core security framework approving or denying the user's access to the requested data based on the security information; and

upon approval, the second enterprise sending the requested data to the user.

25. The method of claim 24 wherein the security information added to the data request is the user ID and password used by the user to log in to the secure computing domain within the first enterprise.

26. The method of claim 24 wherein the security information added to the data request is a token agreed upon by the two enterprises to designate a legitimate data request from the first enterprise to the second enterprise.

27. The method of claim 24 wherein data requests from the user and data returned to the user are in a format compliant with SOAP.

28. The method of claim 24 wherein the data request comprises the selection of a hyperlink on a secure web site within the first enterprise that links to a secure web site hosted by the second enterprise.

29. A method for a user within a second enterprise to gain access to data within a first enterprise comprising:

the user logging in to a secure computing domain within the second enterprise;

the user requesting data from the first enterprise;

the second enterprise adding security information to the data request and sending the data request and security information to the first enterprise;

the first enterprise sending the security information to the second enterprise;

a security gatekeeper within the second enterprise intercepting the security information;

the security gatekeeper sending the security information to a core security framework within the second enterprise;

the second enterprise's core security framework approving or denying the user's access to the requested data based on the security information;

upon approval, the second enterprise informing the first enterprise that the user is allowed access to the requested data; and

the first enterprise sending the requested data to the user.

30. The method of claim 29 wherein the security information added to the data request is the user ID and password used by the user to log in to the secure computing domain within the second enterprise.

31. The method of claim 29 wherein the security information added to the data request is a token agreed upon by the two enterprises to designate a legitimate data request from the second enterprise to the first enterprise.

32. The method of claim 29 wherein data requests from the user and data returned to the user are in a format compliant with SOAP.

33. The method of claim 29 wherein the core security framework is also used to control access to URLs within the second enterprise.

34. The method of claim 29 wherein the data request comprises the selection of a hyperlink on a secure web site within the second enterprise that links to a secure web site hosted by the first enterprise.